

REMARKS/ARGUMENTS

Prior to entry of this amendment, claims 1, 2, 4-19 and 21-23 were pending in this application. No claims are amended, canceled or added herein. Therefore, claims 1, 2, 4-19 and 21-23 remain pending in this application. Applicants respectfully request reconsideration of this application for at least the reasons presented below.

As an initial matter, there seems to be some disagreement over the use of the terms and phrases "generating the signature over" and "authenticating the signature over" as used in the claims. Applicant's respectfully submit the following definitions in an effort to more fully explain the arguments. Rather than arguing a limitation that is not present in the claims as the Office Action suggests, Applicants are simply pointing out the specific meaning of the terms as commonly used which is consistent with the way in which the terms are used in the detailed description and claims.

The term "signing", *i.e.*, generating a digital signature over data, has a specific and well-known meaning. Generally, signing data is a process of calculating a signature by applying any of a variety of algorithms and a unique and presumably secure identifier, such as a private, symmetric, or other key, to the data to be signed. The resulting signature can be used to "authenticate" the data as actually being from the sender or originator rather than a third party. This common usage is consistent with the usage of the terms in the claims and specification as demonstrated at least on page 7 of the detailed description in which the signatory group illustrated in FIG. 5 is described. Furthermore, as can be seen from this portion of the detailed description, "generating a signature over" means calculating a signature using the designated data, in this case, the first data and the second data. "Generating a signature over" does not here mean calculating a signature with one piece of data and using that signature to implicitly authenticate a second piece of data.

"Hashing" is distinct from signing in that it does not identify or authenticate the originator of the data. Rather, hashing is used to identify or verify the contents of the data itself. Similarly, a "message digest" is one or more hash values representing and used for the purpose of identifying or verifying the contents of data. While hashing and signing can in fact be accomplished with similar algorithms, hashing is not performed using a unique identifier, such as a key, for the originator of the data. Rather hashing is simply a matter of applying the hash function to the data to be hashed. The resulting hash value can then be used to verify the contents of the data, i.e., that the data has not been tampered with or otherwise changed. Hashing does not authenticate the originator of the data as signing does. Hence, the distinct terms.

The references cited in the Office Action use a combination of hashing and signing in which data is hashed and then the hash value is signed. In this way, the hash value(s) can be authenticated and the data, if verified by the hash value, can be implicitly authenticated. However, as previously stated, the references do not teach or suggest "generating the signature over" first and second data or "authenticating the signature over" first and second data. Therefore, with these definitions and distinctions in mind, the Applicants restate the previously presented arguments.

35 U.S.C. §102 Rejection, Gennaro et al.

The Office Action has rejected claims 1 and 8 under 35 U.S.C. §102(b) as being anticipated by the cited portions of Non-Patent Literature document "How to Sign Digital Streams" of Gennaro et al. (hereinafter "Gennaro"). The Applicant respectfully submits the following arguments pointing out significant differences between claims 1 and 8 submitted by the Applicant and Gennaro.

As previously stated, Gennaro describes: 1) splitting a stream into blocks; 2) hashing each block and storing the hash value in a table; 3) signing the table; and 4) sending the

signed table followed by the stream. It should be noted that the individual blocks are not signed, only the table is signed. In fact, the table of cryptographic hashes is created and signed "instead of signing each block" further indicating that only the table is signed.

Gennaro does not disclose "generating the signature over" first and second data or "authenticating the signature over" first and second data.. Under Gennaro, a signature is generated over only the hash table. The signed table can be authenticated based on the signature and the contents of the packets can be verified based on the hash values in the table. That is, the packets are implicitly authenticated if they are verified with the hash value. Gennaro does not disclose generating a signature over a first information and a second information as recited in claim 1 or authenticating the signature over the first and second information as recited in claim 8. For at least these reasons, the Applicant requests that the rejection be withdrawn.

35 U.S.C. §102 Rejection, Wong et al.

The Office Action has rejected claims 1 and 8 under 35 U.S.C. §102(e) as being anticipated by the cited portions of Non-Patent Literature document "Digital Signatures for Flows and Multicasts" of Wong et al. (hereinafter "Wong"). The Applicant respectfully submits the following arguments pointing out significant differences between claims 1 and 8 submitted by the Applicant and Wong.

The methods described in Wong are not unlike those described in Gennaro in that only a single piece of data is signed. In Gennaro, only the table of hash values is signed. In Wong, packets are successively hashed and the resulting single message digest is signed. Wong does not disclose generating a signature over a first information and a second information as recited in claim 1 or authenticating the signature over the first and second information as recited in claim 8. For at least these reasons, the Applicant requests that the rejection be withdrawn.

35 U.S.C. §102 Rejection, Wasilewski'474

The Office Action has rejected claims 1-2, 4-6, 8-9, 11-13 and 21 under 35 U.S.C. §102(e) as being anticipated by the cited portions of U.S. Patent No. 5,870,474 of Wasilewski et al. (hereinafter "Wasilewski '474"). The Applicant respectfully submits the following arguments pointing out significant differences between claims 1-2, 4-6, 8-9, 11-13 and 21 submitted by the Applicant and Wasilewski '474.

As previously stated, Wasilewski describes a series of successive encryptions in which a first key is used to encrypt a packet, a second key is used to encrypt the first key, and the customer's public key is used to encrypt the second key. Of these keys, Wasilewski applies a digital signature only to the second key. The encryption of the first key with the multi-session key (MSK) and the encryption of the second key with the user's public key control access to the content but do not affect a signature, only the second key is signed. Therefore, Wasilewski does not disclose generating a signature over a first information and a second information as recited in claim 1, or authenticating the signature over the first and second information as recited in claim 8, or authorization information, wherein: a signature is generated over an information object and the authorization information as recited in claim 14. For at least these reasons, the Applicant requests that the rejection be withdrawn and claims 1-2, 4-6, 8-9, 11-13 and 21 be allowed.

35 U.S.C. §103 Rejection, Wasilewski '474 in view of Banker et al.

The Office Action has rejected claims 7, 10, 14-15 and 19 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of U.S. Patent No. 5,247,364 of Banker et al. (hereinafter "Banker"). The Applicant respectfully submits that the Office Action does not establish a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

In order to establish a *prima facie* case of obviousness, the Office Action must establish: 1) some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine their teachings; 2) a reasonable expectation of success of such a modification or combination; and 3) a teaching or suggestion in the cited prior art of each claimed limitation. See MPEP §706.02(j).

As will be discussed in detail below, the references cited by the Office Action do not teach or suggest each claimed limitation. More specifically, the references, alone or in combination, fail to teach or suggest "generating the signature over" first and second data or "authenticating the signature over" first and second data.

As discussed above, independent claim 1, upon which claim 7 depends, claim 8, upon which claim 10 depends, and claim 14, upon which claims 15 and 19 depend, are distinguishable from Wasilewski. Specifically, Wasilewski does not teach or suggest generating a signature over a first information and a second information as recited in claim 1, authenticating the signature over the first and second information as recited in claim 8, or authorization information, wherein a signature is generated over an information object and an authorization information as recited in claim 14.

Banker is directed to "a method and apparatus for tuning channels in a subscription television system having in-band data transmissions." (Col. 1, lines 10-12) Under Banker, an "addressable transmitter transmits data to out-of-band subscriber terminals via a dedicated FM data channel." (Col. 2, lines 55-57) "Scramblers are coupled to headend controller and may be used to selectively scramble television signals for improved security in a subscription television system that is equipped with appropriate descramblers." (Col. 3, lines 47-51) However, Banker does not teach or suggest generating a signature over a first information and a second information as recited in claim 1, or authenticating the signature over the first and

second information as recited in claim 8, or authorization information, wherein a signature is generated over an information object and the authorization information as recited in claim 14.

The combination of Wasilewski '474 and Banker is no more relevant to the pending claims than either reference alone. Neither Wasilewski '474 nor Banker, alone or in combination, teach or suggest generating a signature over a first information and a second information as recited in claim 1, or authenticating the signature over the first and second information as recited in claim 8, or authorization information, wherein a signature is generated over an information object and the authorization information as recited in claim 14. Therefore, the references cited in the Office Action fail to teach or suggest each claimed limitation. For at least these reasons, claims 7, 10, 14-15 and 19 should be allowed.

35 U.S.C. §103 Rejection, Wasilewski '474 in view of Banker et al. further in view of Shear et al.

The Office Action has rejected claims 16 and 17 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of Banker and further in view of the cited portions of U.S. Patent No. 6,157,721 of Shear et al. (hereinafter "Shear"). The Applicant respectfully submits that the Office Action has not established a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As discussed above, independent claim 14 upon which claims 16 and 17 depend is distinguishable from Wasilewski '474 and Banker since neither Wasilewski '474 nor Banker, alone or in combination, teach or suggest authorization information, wherein a signature is generated over an information object and the authorization information as recited in claim 14.

Shear is directed to "computer security techniques based at least in part on cryptography, that protect a computer processing environment against potentially harmful

computer executables, programs and/or data; and to techniques for certifying load modules such as executable computer programs or fragments thereof as being authorized for use by a protected or secure processing environment." (Col. 1, lines 22-28) Under Shear, "a verifying authority can digitally sign a load module or other executable with several different digital signatures and/or signature schemes." (Col. 7, lines 9-11) That is, "a protected processing environment or other secure execution space may require a load module or other executable to present multiple digital signatures before accepting it." (Col. 7, lines 11-14) In other words, the module may be signed multiple times. However, Shear does not disclose a signature covering more than one module. Therefore, Shear does not teach or suggest authorization information, wherein a signature is generated over an information object and the authorization information.

The combination of Wasilewski '474, Banker, and Shear is no more relevant to the pending claims than any of the references alone. None of the references, alone or in combination, teach or suggest authorization information, wherein a signature is generated over an information object and the authorization information. Therefore, the references cited in the Office Action fail to teach or suggest each claimed limitation. For at least these reasons, claims 16 and 17 should be allowed.

35 U.S.C. §103 Rejection, Wasilewski '474 in view of Banker et al. further in view of Wasilewski '866

The Office Action has rejected claim 18 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of Banker and further in view of the cited portions of U.S. Patent No. 5,420,866 of Wasilewski (hereinafter "Wasilewski '866"). The Applicant respectfully submits that the Office Action has not established a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As discussed above, independent claim 14 upon which claim 18 depends is distinguishable from Wasilewski '474 and Banker since neither Wasilewski '474 nor Banker, alone or in combination, teach or suggest authorization information, wherein a signature is generated over an information object and the authorization information.

Wasilewski '866 "is directed to methods for providing conditional access information to decoders in a packet-based multiplexed communications system." (Col. 5, lines 31-33) Wasilewski teaches "methods for providing a plurality of different sets of conditional access information to a remote location and for facilitating access to a selected one of those sets of conditional access information by a decoder at the remote location." (Col. 5, lines 38-43) In other words, Wasilewski teaches encryption of information for controlling access to information but not signatures over that information. Therefore, Wasilewski '866 does not teach or suggest authorization information, wherein a signature is generated over an information object and the authorization information.

The combination of Wasilewski '474, Banker, and Wasilewski '866 is no more relevant to the pending claims than any of the references alone. None of the references, alone or in combination, teach or suggest authorization information, wherein a signature is generated over an information object and the authorization information. Therefore, the references cited in the Office Action fail to teach or suggest each claimed limitation. For at least these reasons, claim 18 should be allowed.

35 U.S.C. §103 Rejection, Wasilewski et al. in view of Shear et al.

The Office Action has rejected claims 22 and 23 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of Shear. The Applicant respectfully submits that the Office Action has not established a *prima*

Appl. No. 09/493,984
Amdt. dated: October 5, 2005
Amendment under 37 CFR 1.116 Expedited Procedure
Examining Group 2134

PATENT

facie case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

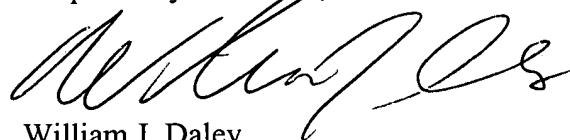
As discussed above, independent claim 14 upon which claims 22 and 23 depend is distinguishable from Wasilewski '474 and Shear since neither Wasilewski '474 nor Shear, alone or in combination, teach or suggest authorization information, wherein a signature is generated over an information object and the authorization information. Therefore, the references cited in the Office Action fail to teach or suggest each claimed limitation. For at least these reasons, claims 16 and 17 should be allowed.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,



William J. Daley
Reg. No. 52,471

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000 (Denver office)
Fax: 303-571-4321 (Denver office)

WJD:sbm

60593196 v1